IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

LIONRA TECHNOLOGIES LIMITED,	
Plaintiff,	Case No. 2:22-cv-00322-JRG (Lead)
vs.	
FORTINET, INC.,	**JURY TRIAL DEMANDED**
Defendant.	[redacted]

DEFENDANT FORTINET, INC.'S MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. § 101

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. STATEMENT OF THE ISSUES TO BE DECIDED BY THE COURT 1

III. STATEMENT OF UNDISPUTED MATERIAL FACTS 1

A. ’612 Patent 1

B. ’436 Patent 2

IV. LEGAL STANDARD 4

V. THE ASSERTED CLAIMS DO NOT RECITE PATENT ELIGIBLE SUBJECT MATTER 5

A. The ’612 Patent 6

1. Step 1: Claim 1 of the ’612 Patent is Directed to an Abstract Idea 6

2. Step 2: Claim 1 of the ’612 Patent Does Not Recite an Inventive Concept 10

a. The Claim Elements 11

b. The Specification Confirms The Lack of an Inventive Concept In the Claims 14

c. The Inventor Testimony Confirms That There Is No Inventive Concept in the Claims 16

d. Plaintiff’s Technical Expert Did Not Identify An Inventive Concept 20

3. The ’612 Patent Asserted Dependent Claim is Also Patent Ineligible 22

B. The ’436 Asserted Claim 23

1. Claim 1 Is Directed to an Abstract Idea 23

2. Claim 1 Does Not Recite an Inventive Concept 24

TABLE OF AUTHORITIES

Cases

Affinity Labs of Tex. v. DIRECTV, LLC, 838 F.3d 1253 (Fed. Cir. 2016).................................... 4

Alice Corp. v. CLS Bank Int'l, 573 U.S. 208 (2014)...............................1, 4, 6, 10-11, 16, 21-22

Berkheimer v. HP, Inc., 881 F.3d 1360 (Fed. Cir. 2018)... 11

BSG Tech LLC v. Buyseasons, Inc., 899 F.3d 1281 (Fed. Cir. 2018)................................. 11, 21

Celotex Corp. v. Catrett, 477 U.S. 317 (1986) 4

ChargePoint, Inc. v. SemaConnect, Inc., 920 F.3d 759 (Fed. Cir. 2019) 21

Dropbox, Inc. v. Synchronoss Techs., Inc., 815 F. App'x 529 (Fed. Cir. 2020).......... 4, 7, 13, 23

FairWarning IP, LLC v. Iatric Sys., Inc., 839 F.3d 1089 (Fed. Cir. 2016) 7

First-Class Monitoring, LLC v. United Parcel Serv. of Am., Inc., 389 F. Supp. 3d 456 (E.D. Tex. 2019) 6

Mobile Telecomm'cns Techs., LLC v. Blackberry Corp., No. 3:12-cv-1652-M, 2016 WL 2757371 (N.D. Tex. May 12, 2016) 19

RecogniCorp, LLC v. Nintendo Co., 855 F.3d 1322 (Fed. Cir. 2017) 11, 23

REGENXBIO Inc. v. Sarepta Therapeutics, Inc., No. CV 20-1226-RGA, 2024 WL 68278 (D. Del. Jan. 5, 2024)... 13, 16, 19

Semantic Search Techs. LLC v. Aldo U.S., Inc., 425 F. Supp. 3d 758 (E.D. Tex. 2019) 4

Tokai Corp. v. Easton Enters., Inc., 632 F.3d 1358 (Fed. Cir. 2011)... 4

Universal Secure Registry LLC v. Apple Inc., 10 F.4th 1342 (Fed. Cir. 2021) 9-10

Statutes

35 U.S.C. § 101...1, 6, 19-21

Other Authorities

ARPANET, Defense Advanced Research Projects Agency, https://www.darpa.mil/about-us/timeline/arpanet (last visited Feb. 20, 2024).................... 12

FED. R. CIV. P. 56(a).. 4

U.S. Patent No. 7,424,744 14

I. INTRODUCTION

Claim 1 of the ’436 Patent and Claims 1 and 12 of the ’612 Patent (the “Asserted Claims”) are invalid under 35 U.S.C. § 101 because they fail the two-step *Alice* test. First, the Asserted Claims are directed to the abstract idea of sending and receiving messages. This includes the basic actions of sorting messages by some criteria, decrypting a message if necessary, and checking whether a message contains certain key words—all analogous to actions that have been performed by humans for decades. Second, the Asserted Claims do not recite an inventive concept sufficient to transform the abstract idea into patent-eligible matter. In fact, Plaintiff’s interpretation of the Asserted Claims (from which it argues infringement) confirms that the Asserted Claims are directed to an abstract idea and lack inventive concept. As confirmed by the testimony of inventor John Davis, the invention that the Asserted Claims were intended to capture cannot actually be found anywhere in the claims. This is particularly true as a result of Plaintiff’s infringement positions after accounting for the claim constructions. Likewise, Plaintiff’s validity expert (Dr. Eric Cole), could not salvage the claims in this regard. Defendant Fortinet, Inc., therefore, respectfully asks the Court to grant summary judgment that the Asserted Claims are invalid.

II. STATEMENT OF THE ISSUES TO BE DECIDED BY THE COURT

Whether the Asserted Claims are invalid under 35 U.S.C. § 101.

III. STATEMENT OF UNDISPUTED MATERIAL FACTS

A. ’612 Patent

1. The ’612 Patent is titled “System and method for a secure I/O interface,” Dkt. 1-4 at 1 (Cover Page), and the Asserted Claims of this patent are 1 (independent) and 12 (depends from Claim 1). Ex. G at ¶ 12.

2. The ’612 Patent identifies two inventors: John M. Davis and Richard Takahashi. Dkt. 1-4 at 1 (Cover Page).

3. The ’612 Patent issued on October 22, 2013, and Plaintiff asserts that the priority date is October 2, 2003. Dkt. 1-4 at 1 (Cover Page); Ex. A at ¶ 127.

4. The preamble of Claim 1 recites a “security processor to process incoming packets and outgoing packets, the security processor comprising.” *See* Dkt. 1-4 at [1pre]. The remainder of the claim describes the “processing” of the “incoming packets” and “outgoing packets”:

> [1pre] A security processor to process incoming packets and outgoing packets, the security processor comprising:
>
> [1a] a switching system to send the outgoing packets and receive the incoming packets;
>
> [1b] a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines;
>
> [1c] a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
>
> [1d] a signature database; and
>
> [1e] an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

Dkt. 1-4 at 20:54-21:12 (cl. 1).

B. ’436 Patent

5. The ’436 Patent is also titled “System and method for a secure I/O interface,” Dkt. 1-2 (’436 Patent) at Cover Page, and the only Asserted Claim of the ’436 Patent is Claim 1, an independent claim. Ex. G at ¶ 12.

6. The ’436 Patent issued on March 23, 2010, and Plaintiff asserts that the priority date is October 2, 2003: October 2, 2003. Dkt. 1-2 at Cover Page; Ex. A, Almeroth Report at ¶ 127. The ’436 Patent largely shares the same specification as the ’436 Patent. *Compare* Dkt. 1-4 *with* Dkt. 1-2.

7. The ’436 Patent identifies the same two inventors as the ’612 Patent: Davis and Takahashi.

8. Claim 1 of the ’436 Patent recites:

> [1pre] A security processor to process incoming packets and outgoing packets, the security processor comprising:
>
> [1a] a switching system to send the outgoing packets and receive the incoming packets;
>
> [1b] a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and
>
> *[1c] wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core*;
>
> [1d] a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
>
> [1e] a signature database; and

> [1f] an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

Dkt. 1-2 at 24:10-39.

9. Claim 1 is identical to Claim 1 of the ’612 Patent, except for the italicized language in element [1c].

IV. LEGAL STANDARD

Summary judgment is warranted when “there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” FED. R. CIV. P. 56(a); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). “Summary judgment is as available in patent cases as in other areas of litigation.” *Tokai Corp. v. Easton Enters., Inc.*, 632 F.3d 1358, 1366 (Fed. Cir. 2011).

The two-step analytical framework for evaluating patent eligibility is set forth in *Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208 (2014). Three legal points bear emphasis for this motion.

First, patents claiming data formatting and transmission, even if limited to a field of use, are particularly susceptible to being drawn to abstract ideas, regardless of the technological field. *Dropbox, Inc. v. Synchronoss Techs., Inc*., 815 F. App’x 529, 537 (Fed. Cir. 2020).

Second, an alleged “inventive concept” must be recited in the claims themselves. *Semantic Search Techs. LLC v. Aldo U.S., Inc.*, 425 F. Supp. 3d 758, 777 (E.D. Tex. 2019).

Third, limiting a patent claim to a field of use, such as a particular type of network system in the Asserted Patents, does not add the required level of specificity or concreteness. *See, e.g., Affinity Labs of Tex. v. DIRECTV, LLC*, 838 F.3d 1253, 1259 (Fed. Cir. 2016) (“The Supreme Court and this court have repeatedly made clear that merely limiting the field of use of the abstract idea to a particular existing technological environment does not render the claims any less abstract.”).

V. THE ASSERTED CLAIMS DO NOT RECITE PATENT ELIGIBLE SUBJECT MATTER

The Asserted Claims disclose the conventional concepts of a switching system to send and receive packets, a component to classify (in no particular way) and tag packets to help direct them, a component that encrypts or decrypts packets (again in no particular way), and a component that matches signatures in packets (also in no particular way and does not have to actually do anything if there is a match). Dkt. 1-2, 1-4.

In this case, the concepts of the system described above are accomplished by the claimed "switching system," "database," "packet engine," "cryptographic core," and "intrusion detection system." Based on the Court's claim constructions, the "packet engine," "cryptographic core," and "intrusion detection system" can be conventional processing hardware—for example, a general-purpose CPU running software. Dkt. 162 at 37-38, 41-42, 44-46. Specifically, the Court found that these components can be satisfied by hardware or hardware in combination with software. Dkt. 162 at 37-38, 41-42, 44-46. According to the Court's claim construction order, therefore, these components do not need to be implemented in distinct hardware components, but can be implemented using a single general-purpose CPU running software. Dkt. 162 at 37-37, 41-42, 44-46. And Plaintiff's validity expert, Eric Cole, testified that he did not opine on whether these components had to be physically connected. Ex. B, Cole Dep. Tr. (Rough Feb. 9, 2024) at 216:13-25.

The alleged "inventive concept" must be recited in the claims themselves, but in this case, the Asserted Claims, both individually and as a combination, do not provide such a concept. Instead, they merely recite well-understood, routine, and conventional components and activities that were well known to a POSITA before the priority date of the Asserted Patents. Aside from the abstract idea, all of the system components and processing steps recited in the Asserted Claims were known in the art, and merely describe conventional computing components and techniques. Because the Asserted Claims are directed to an abstract idea and because the claims recite conventional limitations that were already known in the art and do not provide an inventive concept, the Asserted Claims are directed to patent ineligible subject matter and therefore invalid under 35 U.S.C. § 101.

A. The ’612 Patent

Plaintiff has narrowed the asserted claims of the ’612 Patent to claims 1 (independent) and 12 (depends from Claim 1). *See* Section IV.B.

1. <u>Step 1</u>: Claim 1 of the ’612 Patent is Directed to an Abstract Idea

At step 1, the Court examines the focus of the claim to determine whether it is directed to an abstract idea. Federal courts have characterized "method[s] of organizing human activity" as abstract. *First-Class Monitoring, LLC v. United Parcel Serv. of Am., Inc.*, 389 F. Supp. 3d 456, 462 (E.D. Tex. 2019). Thus, if a "'claimed invention only performs an abstract idea on a generic computer, the invention is directed to an abstract idea at step one' of *Alice*." *Id.* (quoting *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1285 (Fed. Cir. 2018)). The "fact that a computer can perform such operations more rapidly and efficiently [does not] make an abstract idea any less abstract or any more patent-eligible." *Id.* "In the computer field, this principle has sometimes been described as requiring 'a technological solution to a technological problem specific to computer networks.'" *Id.* at 463 (quoting *Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1301 (Fed. Cir. 2016)); *see also id.* (citing *In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 613 (Fed. Cir. 2016) ("the claims are not directed to a solution to a 'technological problem'")).

Claim 1 is directed to a series of abstract ideas, such as (1) receiving and sending out information (like a clerk receiving and sending messages); (2) decrypting received information or encrypting outgoing information (like decoding a confidential message after receiving it, or encoding a confidential message before sending it out); (3) classifying information (like sorting messages by subject matter); and (4) determining whether the information contains certain things on a list (like checking whether the message contains certain words or phrases on a list of key words/phrases). These basic tasks have been executed by humans long before this patent, and Claim 1 is not directed to a technical solution for a technological problem. *See* Ex. A at Section XIII. Each claim element is discussed below.

Element 1[a]. This element is directed to sending and receiving information, and it does not provide any technical details as to how the sending and receiving of packets is to be accomplished. Dkt. 1-4 at 20:56-57. It is a quintessential example of an abstract concept. *See, e.g.*, *Dropbox*, 815 F. App'x at 537 (evaluated patent claims that performed data backups by "[f]ormatting data, tagging data, transmitting data, and retrieving data" and found them drawn to ineligible abstract ideas).

Element 1[b]. This element is directed to the plurality of packet engines coupled to the switching system and handling classification processing of the incoming and outgoing packets. It does not include any details about how the "classification processing" is accomplished, nor does it specify how "substantially all of the incoming and outgoing packets" are determined. There is nothing in Claim 1 that provides a specific means or method to improve classifying information. *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1095 (Fed. Cir. 2016). Indeed, humans have been able to classify messages or information, at least since pen and paper first created written messages hundreds of years ago. Simply reading messages and then sorting them by subject matter were basic tasks of reading comprehension. Even in the realm of the Internet, data packets have been sent and received since well before the priority date of the Patents-in-Suit. *See FairWarning*, 839 F.3d at 1094-95 (claims abstract where language asked "same questions (though perhaps phrased with different words) that humans in analogous situations detecting fraud have asked for decades, if not centuries").

The *Markman* Order reinforced that the classification recited in this element is abstract. The Court construed "substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines" in Element [1b] to have its plain meaning. The Court noted that the "substantially all . . ." limitation expresses that not every packet passes through the packet engines. Dkt. 162 at 33. The Court construed "packet engine" to mean "hardware, or a combination of hardware and software, that is configured to perform packet operations." Dkt. 162 at 39. These constructions do not provide any inventive requirements about what type of "classification processing" is required, how it is accomplished, or how "substantially all of the incoming and outgoing packets" are determined. *See* Dkt. 162 at 33, 39. They likewise do not require any specific hardware implementation of a "packet engine." Moreover, Claim 1 does not disclose any technical details or solutions regarding coupling to the packet engine, receiving packets, communicating outgoing packets, or providing encryption or decryption processing.

Element 1[c]. This element is directed to the cryptographic core coupled to the packet engine and providing encryption and decryption processing for the packets received from and sent to the packet engine. The Court construed "cryptographic core" to mean "hardware, or a combination of hardware and software, that is configured to perform cryptographic processing." Dkt. 162 at 42. The construction does not include any technical requirements about the "cryptographic core" or how it is implemented, and the claim itself does not disclose any technical details or solutions regarding coupling to the packet engine, receiving packets, communicating outgoing packets, or providing encryption or decryption processing. Further, there is nothing in the claims or the specification that provides any specific means or method to improve encryption and decryption. In fact, decryption and encryption, even in complex forms, are simply mathematical operations, and messages have been encoded and decoded long before computers even existed. Ex. A at Section XIII.

Element 1[d]. This element is directed to a signature database. It does not require any specific implementation details of the signature database, any specific way or details regarding how signatures are matched to packets, or any specific hardware configuration for the intrusion detection system. In fact, the claim does not even require any specific action upon a signature match. If a patentee claims that an invention constitutes a technological improvement, the improvement must be in the claims with sufficient specificity such that it is not abstract. *See Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1346 (Fed. Cir. 2021).

Element 1[e]. This element is directed to an intrusion detection system coupled between the cryptographic core and the packet engine. The claim language does not provide any details about what the intrusion detection system is—other than a system that detects intrusions in some way. Nor does it provide what it means for the intrusion detection system to be responsive to a packet matching a signature. Plaintiff's validity expert, Eric Cole, also could not articulate how the claim language improved the communication system. *See, e.g.,* Ex. B at 219-22.

Likewise, matching key words or phrases in a message is rooted in the basic human operation of reading. Ex. A at Section XIII. For example, a clerk may have been instructed to identify any messages that contain the phrases "past due invoice" or "overdue invoice" or to find any messages from "Jon Doe" or "Jane Doe." There is nothing in Claim 1 that provides a specific means or method to improve "signature matching" in the received information, and in fact, Claim 1 does not even specify any specific operation that must happen in the event of a signature match.

The Court construed "intrusion detection system" to mean "hardware, or a combination of hardware and software, that is configured for matching parts of a data stream against a stored set of patterns." Dkt. 162 at 46. This construction does not reflect a technical requirement about the "intrusion detection system," nor how it is implemented. Instead, matching an incoming data stream (which is the essence of any received communication in a computer network) with a stored set of patterns is—at the level claimed and construed—purely abstract.

<u>Summary</u>. Lionra's infringement expert, Dr. Hugh Smith, confirmed that—according to Plaintiff's infringement theory—Claim 1 does not have any technical requirements other than that software accomplishes all of these features (again, the classic example of an abstract idea):

> [redacted]
>
> [redacted]

Smith Dep. Tr. at 93:22-94:5 (Rough Feb. 14, 2024). Claim 1 of the '612 Patent is directed to processing packets "for which computers are merely used in a conventional way, rather than a technological improvement to computer functionality itself." *Universal Secure Registry*, 10 F.4th at 1350. Because "claims must recite a specific means or method that solves a problem in an existing technological process," Claim 1 is instead directed to an abstract idea under the first step of *Alice*.

2. <u>Step 2</u>: Claim 1 of the '612 Patent Does Not Recite an Inventive Concept

The second step of the *Alice* framework does not rescue Claim 1 from patent ineligibility. At *Alice* step two, courts look for an "inventive concept" and "consider the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent eligible application. The second set of the *Alice* test is satisfied when the claim limitations involve more than the performance of well-understood, routine, [and] conventional activities previously known in the industry." *Berkheimer v. HP, Inc.*, 881 F.3d 1360, 1367 (Fed. Cir. 2018) (cleaned up). "To save a patent at step two, an inventive concept must be evident in the claims." *RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1327 (Fed. Cir. 2017).

Here, there is no material fact dispute regarding the answer to the "inventive concept" question at *Alice* step two—particularly in light of the positions Lionra and its expert Dr. Smith have taken concerning the breadth of Claim 1. "Whether a combination of claim limitations supplies an inventive concept that renders a claim 'significantly more' than an abstract idea to which it is directed is a question of law." *BSG Tech LLC*, 899 F.3d at 1290. Although underlying "factual determinations may inform this legal determination," *id.*, courts have recognized that it can be decided "as a matter of law" where "there is no genuine issue of material fact." *Berkheimer*, 881 F.3d at 1368.

This Court can readily determine, as a matter of law, that nothing in the claim limitations, taken individually or as an ordered combination, adds "significantly more" to the abstract idea in Claim 1 of the '612 Patent. The claim elements, individually and in combination, merely recite well-understood, routine, and conventional components and activities previously known in the field to a POSITA before the priority date of the '612 Patent.

a. The Claim Elements

Again, Claim 1 of the '612 Patent requires that the claimed "security processor" be made up of the following elements: [1a] "a switching system," [1b] "a packet engine," [1c] "a cryptographic core," [1d] "a signature database," and [1e] "an intrusion detection system."

Element 1[a]. "[S]witching system" has not been construed by the Court. The language in Element [1a] only specifies that the "switching system" "send[s] the outgoing packets and receive[s] the incoming packets." Otherwise, the claim does not provide any technical details as to how the sending and receiving of packets are to be accomplished. Dkt. 1-4 at 20:56-57. Switches that send outgoing packets and receive incoming packets, per the claim language, were well-known, conventional components well before the priority date of the '612 Patent. Mimicking the century-old structure of the switched public telephone system, switches have been used in Internet communication since the early days of the Internet. *See* Ex. A at Section XIII.A. 1, 2 & 4. For example, Cisco has been selling its Catalyst line of switches since at least 1996. *Id.* at ¶ 137. Indeed, the first packet-switched network dates back to 1969, when ARPANET was initially demonstrated. *ARPANET*, Defense Advanced Research Projects Agency, https://www.darpa.mil/about-us/timeline/arpanet (last visited Feb. 20, 2024). There is no disclosure in the claim that the "switching system" is anything other than a conventional switch that sends and receives packets. Inventor Davis admitted that there was nothing inventive about network switches, which he acknowledged have been known since at least the early nineties:

[redacted]

[redacted]

Ex. D, Davis Dep. Tr. at 38:18-38:22 (Dec. 18, 2023).

Element 1[b]. Also, looking at the Court's analysis of the constructions for "packet engine," "cryptographic core," and "intrusion detection system" (Elements [1b], [1c], and [1e] respectively), the Court "expressly rejected"—at Plaintiff's behest—that the "packet engine," "cryptographic core," and "intrusion detection system" must be "distinct, separate hardware." Dkt. 162 at 37 – 46. Thus, each of these components can be implemented in the same "combination of hardware and software." In other words, based on Plaintiff's apparent view of the Asserted Claims (e.g., from its infringement expert), each of these components can simply be a general-purpose processor running software. *See* Ex. C at 93:22-94:5; *see also REGENXBIO Inc. v. Sarepta Therapeutics, Inc.*, No. CV 20-1226-RGA, 2024 WL 68278, at *6 (D. Del. Jan. 5, 2024) (disagreeing with plaintiff's arguments in support of eligibility in part because of plaintiff's interpretation of the scope of the claims through its expert who opined the claims did not have the use articulated by plaintiff).

Element 1[c]. *See* Element 1[b], *supra*.

Element 1[d]. The Court did not construe "signature database" in element [1d]. The specification explains that the "[s]ignature database 304 is a defined set of patterns stored in on and/or off-chip memory." Dkt. 1-4 at 18:43-45. There is nothing in the claims showing that there is anything inventive about using a conventional database. The claim does not require any specific implementation details of the signature database, any specific way or details regarding how signatures are matched to packets, or any specific hardware configuration for the intrusion detection system; in fact, the claim does not even require any specific action upon a signature match. *See, e.g., Dropbox*, 815 F. App'x at 537 (patent claims that performed data backups by "[f]ormatting data, tagging data, transmitting data, and retrieving data" drawn to ineligible abstract ideas). Thus, a POSITA would understand that the "signature database" is simply a well-known, conventional database that stores signatures. Ex. A at Section XIII.A.2.

Again, there is no dispute about these basic facts. Databases, including "signature databases," were around long before the priority date of the '612 Patent, as inventor Davis confirmed:

> [redacted]
>
> [redacted]
>
> [redacted]
>
> [redacted].

Ex. D, Davis Dep. Tr. at 41:2-42:4. As another example, a patent filed in 2002 explained that already in 2002, "Conventional signature based network intrusion detection systems treat signatures as passive items. When a packet is inspected, it is matched against a list of signatures." Ex. E, U.S. Patent No. 7,424,744 at 2:11-13.

Element 1[e]. *See* Element 1[b], *supra*.

b. The Specification Confirms The Lack of an Inventive Concept In the Claims

The aspects of the specification that describe the claimed embodiment confirms that there is no technical solution in the clams. The '612 Patent describes the problem to solve as follows: "a general need for a secure I/O interface system and method that improve the security of communications to and from trusted hardware, improve communication speed, reduce the number of different systems required for secure communications, and reduce the extent of the bottleneck on the backplane bus." Dkt. 1-4 at 2:21–26. Figure 2 illustrates an architecture for implementing the system:

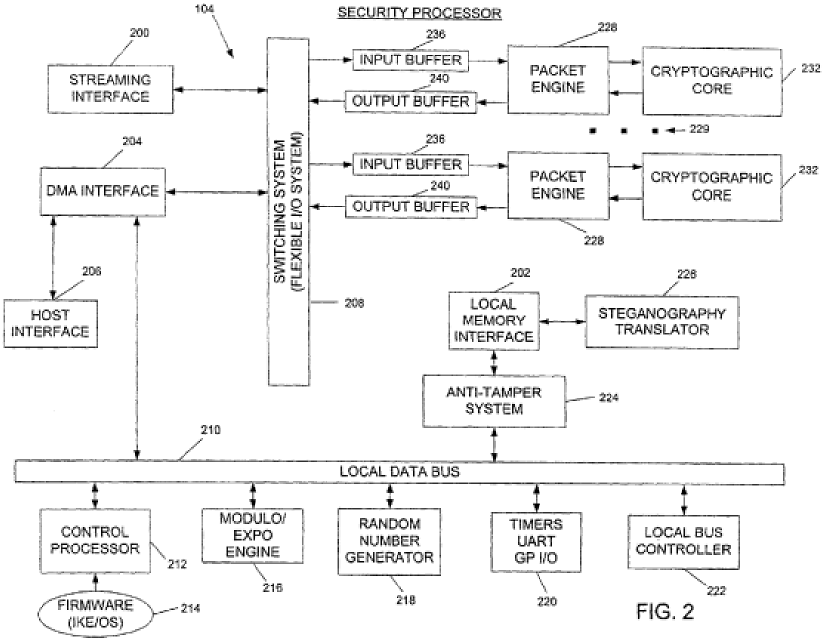

FIG. 2

’612 Patent, Figure 2.

Referring to this figure, the claimed security processor includes a switching system 208 (6:54, 6:58-61), packet engines 228 (7:4-6, 7:13-18) interposed between the switching system and cryptographic cores, cryptographic core 232 (9:60-62), intrusion detection system 302 (18:34-43), and signature database 304 (18:35-39). The switching system provides a mechanism to route packets and data in the security processor, *id.* 6:58-61, and all packet data flows to a packet engine and then to a corresponding cryptographic core, *id.* 20:2-6. The packet engines receive packets from the switching system that are used for packet processing and classification, and the packet engine forwards the packets to a cryptographic core. *Id.* 9:60-64, 10:8-13, 10:58-63, 11:9-16, 11:48-64, 20:4-14. The cryptographic core provides security processing, including encryption and decryption. *Id.* Abstract, 11:27-29, 11:55-59, 20:32-38. The security processor also includes an intrusion detection system (“IDS”) and signature database that are coupled between the packet engine and the cryptographic core. *Id.* 18:34-38. This description of conventional components does not begin to meet the “significantly more” standard to save the claim at the second step of

Alice. Instead, "[t]hese portions of the specification indicate that the claimed invention is made using well-understood, routine, and conventional steps." *REGENXBIO*, 2024 WL 68278, at *6. And Claim 1 does not provide any detail as to how the claimed security processor improves functionality comprised of the above generic components.

c. The Inventor Testimony Confirms That There Is No Inventive Concept in the Claims

Mr. Davis testified that the concepts of switching (receiving and sending packets), packet classification, encrypting and decrypting packets, and signature matching on packets—in other words, everything actually claimed—were all known in the art. Rather, he testified that what he invented was the specific configuration of these well-known concepts into distinct hardware (i.e., separate portions of a system on chip), arranged in a certain way:

> [redacted]
>
> [redacted]

Ex. D, Davis Dep. Tr. at 33:11-34:3 (emphasis added). Mr. Davis confirmed that the invention was the specific configuration, i.e., the aspect that is not in the claims (especially in view of Plaintiff's expansive infringement theory):

> [redacted]
>
> [redacted].

Ex. D, Davis Dep. Tr. at 42:10-42:15. He summed it up by explaining that his invention was not the "what" (which is all that is in the claims), but the "how" (which is not):

[redacted]

[redacted]

Ex. D, Davis Dep. Tr. 103:18-104:15 (emphasis added). Mr. Davis explained that what he considered inventive about the '612 Patent was the specific arrangement of separate hardware portions of a System on Chip, configured to perform previously known actions in what he believed to be a more efficient and effective manner. He explained System on Chips as follows:

[redacted]

[redacted]

[redacted]

[redacted]

Ex. D, Davis Dep. Tr. at 23:18-24:12 (emphasis added). So, the specific configuration that Mr. Davis considered inventive required that different components of the System on Chip perform the different functions:

[redacted]

[redacted]

Ex. D, Davis Dep. Tr. at 43:17-44:15 (emphasis added). He made clear that the invention he thought was in the claims—for example in the requirement that "the packet engine is interposed between the switching system and the cryptographic core"—required that these different elements be separate hardware components on a System on Chip:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Ex. D, Davis Dep. Tr. at 44:20-46:13 (emphasis added).

In sum, what Mr. Davis considered inventive about the ’612 Patent was the specific arrangement of separate hardware portions of a System on Chip, configured to perform previously-known actions in what he believed to be a more efficient and effective manner. However, as set forth above, the constructions of “packet engine,” “cryptographic core,” and “intrusion detection system” (at Plaintiff’s urging) are that they need <u>not</u> be separate hardware components, and can instead be embodied in a general-purpose processor running software. Thus, in view of Plaintiff’s infringement allegations based upon the claim constructions, the one thing the inventor considered inventive about his patent is not actually claimed in the Asserted Claims. *See Mobile Telecomm’cns Techs., LLC v. Blackberry Corp.*, No. 3:12-cv-1652-M, 2016 WL 2757371, at *3-4 (N.D. Tex. May 12, 2016) (citing inventor testimony as evidence that “the asserted claim of the '506 Patent is directed to a longstanding, well-known practice, rather than a patent-eligible idea”); *REGENXBIO*, 2024 WL 68278, at *3 (granting defendants’ motion for summary judgment on § 101 invalidity, where defendant argued “that the language of the ’617 patent, the testimony of the patent’s inventors, and the testimony of Plaintiffs’ own expert support Defendants’ position”).

d. Plaintiff's Technical Expert Did Not Identify An Inventive Concept

Plaintiff's validity expert, Eric Cole, does not, and could not, articulate an inventive concept in the claim language. His expert report does not articulate how the system components in Claim 1 are arranged to improve communication speeds. Instead, he changes the subject altogether. He improperly relied on his Section 102 and 103 analysis finding the claims are not anticipated or rendered obvious by the identified system art, rather than conducting the analysis required under Section 101. The portion of his analysis on Section 101 that he kept referring to is as follows:

[redacted]

[redacted]

Ex. F at ¶¶ 282-83. When pressed at his deposition to articulate "how," he could not and referred back to his insufficient report: [redacted]" When specifically asked why he had not "[redacted]," Mr. Cole just referred back to ¶ 282: "[redacted]. *See, e.g.*, Ex. B, Cole Dep. Tr. 217:11-218:8 (Feb. 9, 2024).

As a matter of black-letter law on Section 101, the "abstract idea itself . . . cannot supply the inventive concept that renders the invention significantly more." *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 774 (Fed. Cir. 2019); *BSG Tech.*, 899 F.3d. at 1290 ("It has been clear since *Alice* that a claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention 'significantly more' than the ineligible concept."). Here, even if the '612 Patent specification discusses the usefulness of the claimed invention for a switching system, Claim 1 recites the performance of well-understood, routine, and conventional data transmission techniques using the standard format; it does not specify how the components are arranged in a more effective and efficient manner. As a result, Claim 1 does not add anything "significantly more" to the abstract idea at *Alice* step two.

3. The '612 Patent Asserted Dependent Claim is Also Patent Ineligible

Clam 12, the '612 Patent asserted dependent claim, is also patent ineligible because it is directed to an abstract idea and does not recite an inventive concept sufficient to transform the abstract idea into patent eligible subject matter. Claim 12 depends from Claim 1 and requires that "the at least one packet matching the signature stored in the signature database comprises a plain text packet." This claim simply states the abstract idea that the message on which signature matching is performed is "plain text," which a POSITA would understand means it is not encrypted. Thus, the abstract idea explained above in connection with claim 1 of the '612 Patent applies equally here, and there is nothing in claim 12 that adds an inventive concept.

Moreover, Claim 12 of the '612 Patent also does not provide any inventive concept because, aside from the abstract idea discussed above, the claim elements, individually and in combination, merely recite well-understood, routine, and conventional components and activities previously known in the field to a POSITA before the priority date of the '612 Patent. Namely, it was well-known to a POSITA that one would want to decrypt a message before determining if the message contains key words or phrases. Indeed, the '612 Patent itself identifies pre-existing cryptographic cores that were "suitable for use with the present invention." Dkt. 1-4 at 11:29-47. Thus, dependent Claim 12 is directed to the abstract idea set forth above, and does not recite an inventive concept sufficient to transform the abstract idea into patent eligible subject matter.

B. The ’436 Asserted Claim

Claim 1 of the ’436 Patent is directed to the same abstract idea as Claim 1 of the ’612 Patent, and thus, the analysis above also applies here. *See* Section A.1, *supra*. Claim 1 does have an additional wherein clause, but even still, this distinction is not enough to save the claim.

1. Claim 1 Is Directed to an Abstract Idea

Element [1b] has the following additional clause: “wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core.” But this clause is merely analogous to the clerk described above, who is labeling messages with an address or other indicator to show where the messages should go (for example, after being decrypted). *See* Section A.1, *supra*. *See also Dropbox*, 815 F. App’x at 837 (claims drawn to formatting data, tagging data, transmitting data, and retrieving data were abstract). The claim language fails to provide any specific or concrete means for achieving the desired tagging. *See generally* Dkt. 1-2.

Thus, Claim 1 of the ’436 Patent is directed to nothing more than the abstract idea of receiving and sending out information (e.g., a clerk receiving and sending messages), decrypting received information or encrypting outgoing information (e.g., decoding a received message that is encoded, or encoding a confidential message before sending it out), classifying information (e.g., sorting messages by subject matter), adding address information to a message to direct it to the right place, and determining whether the information contains certain things on a list (e.g., whether the message contains certain words or phrases on a list of key words/phrases). Ex. A at Section XIII.B.1 – 2; *see also RecogniCorp, LLC*, 855 F.3d at 1326 (“This method reflects standard encoding and decoding, an abstract concept long utilized to transmit information.”).

2. Claim 1 Does Not Recite an Inventive Concept

Moreover, Claim 1 of the ’436 Patent does not provide an inventive concept sufficient to transform the abstract idea into patent eligible subject matter, even with the additional wherein clause. The claim, like Claim 1 of the ’612 Patent, requires that the claimed “security processor” be made up of the following elements: [1a] “a switching system,” [1b] “a packet engine,” [1c] “a cryptographic core,” [1d] “a signature database,” and [1e] “an intrusion detection system.” As explained above in connection with claim 1 of the ’612 Patent, in view of the Court’s claim construction Order, these elements are well-known, conventional computing components that do not add an inventive concept to the abstract idea. *See* Section V.A.2., *supra;* Ex. A at Section XIII.B.1-2.

The additional wherein clause in element [1b] (“wherein the incoming packets and outgoing packets are provided with a tag . . .”) does not add anything inventive to the claim. Addressing messages (tagging) to assist with delivering them to the right location has been around since well before the priority date of the ’436 Patent. Ex. A at Section XIII.B.1 – 2. Tagging of the packet upon ingress to the packet engine 228 may determine the egress path from cryptographic core 232. More specifically, the incoming and outgoing packets may be provided with a tag upon ingress to one of packet engines 228 and the tag may be used to determine the egress path upon exit from the corresponding cryptographic core 232.” ’436 Patent, 20:13-20. This additional claim limitation does not require additional components and is simply a routine concept that can be implemented by humans. Thus, the elements of Claim 1, individually and in combination, do not recite an inventive concept sufficient to transform the abstract idea into patent eligible subject matter, as described above and in connection with by analysis of claim 1 of the ’612 Patent.

Thus, like Claim 1 of the ’612 Patent, Claim 1 of the ’436 Patent is directed to patent ineligible subject matter.

Dated: February 20, 2024

Respectfully submitted,

/s/ Melissa R. Smith
Melissa R. Smith (TBN 24001351)
melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, TX 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

Matthew C. Gaudet
mcgaudet@duanemorris.com
David C. Dotson
dcdotson@duanemorris.com
John R. Gibson
jrgibson@duanemorris.com
Alice E. Snedeker
aesnedeker@duanemorris.com
Daniel Mitchell
dmitchell@duanemorris.com
DUANE MORRIS LLP
1075 Peachtree Street, N.E., Suite 1700
Atlanta, Georgia 30309-3929
Telephone: 404.253.6900
Facsimile: 404.253.6901

Alexandra A. Lane
axlane@duanemorris.com
DUANE MORRIS LLP
1540 Broadway
New York, NY 10036-4086
Telephone: 212.471.4772
Facsimile: 212.937.3568

Brianna M. Vinci
bvinci@duanemorris.com
DUANE MORRIS LLP
30 S. 17th Street
Philadelphia, PA 19103
Telephone: 215.979.1198
Facsimile: 215.754.4983

Counsel For Defendant
Fortinet, Inc.

CERTIFICATE OF SERVICE

The undersigned counsel hereby certifies that on February 20, 2024, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all attorneys of record.

/s/ Melissa R. Smith
Melissa R. Smith
Counsel for Defendant
Fortinet, Inc.

[redacted]

[redacted]

[redacted]